

**PCT**WELTORGANISATION FÜR GEISTIGES EIGENTUM  
Internationales BüroINTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE  
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

|  |  |  |  |
|--|--|--|--|
| (51) Internationale Patentklassifikation <sup>7</sup> :<br><b>A01K 11/00</b>   |  | A1   | (11) Internationale Veröffentlichungsnummer: <b>WO 00/01227</b>            |
|  |  |  | (43) Internationales<br>Veröffentlichungsdatum: 13. Januar 2000 (13.01.00) |
| (21) Internationales Aktenzeichen: PCT/DE99/01937  |  | (81) Bestimmungsstaaten: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). |  |
| (22) Internationales Anmeldedatum: 30. Juni 1999 (30.06.99)  |  |  |  |
| (30) Prioritätsdaten:<br>198 29 034.9 30. Juni 1998 (30.06.98) DE  |  |  |  |
| (71) Anmelder (für alle Bestimmungsstaaten ausser US): GENER-<br>ATIO GMBH [DE/DE]; Wollgrasweg 9, D-70599 Stuttgart<br>(DE).  |  |  |  |
| (71)(72) Anmelder und Erfinder: MANZ, Eberhard [DE/DE]; Fet-<br>zerstrasse 4, D-70199 Stuttgart (DE).  |  |  |  |
| (74) Anwälte: SCHOHE, Stefan usw.; Boehmert & Boehmert,<br>Hollerallee 32, D-28209 Bremen (DE).  |  | <b>Veröffentlicht</b><br><i>Mit internationalem Recherchenbericht.</i><br><i>Vor Ablauf der für Änderungen der Ansprüche zugelassenen</i><br><i>Frist; Veröffentlichung wird wiederholt falls Änderungen</i><br><i>eintreffen.</i>   |  |
| (54) Title: METHOD FOR DETERMINING THE ORIGIN OF AND/OR IDENTIFYING ANIMALS OR BIOLOGICAL MATERIAL   |  |  |  |
| (54) Bezeichnung: VERFAHREN ZUM NACHWEIS DER ABSTAMMUNG UND/ODER ZUR IDENTIFIZIERUNG VON TIEREN<br>ODER VON BIOLOGISCHEM MATERIAL  |  |  |  |
| (57) Abstract  |  |  |  |
| <p>The invention relates to a method for determining the origin of and/or identifying animals or biological material of animals and organisms. The method comprises the following steps: storing identification data on a data storage medium in the form of an encoded message which has an unequivocal relationship with an item of genetic information unequivocally identifying an animal or the biological material; and checking the identification data to see whether it has said predetermined relationship with the genetic information. The invention also relates to a chip card and a computer system for use in carrying out the method and to a method for generating the data allocated to the animal.</p>                                       |  |  |  |
| (57) Zusammenfassung   |  |  |  |
| <p>Die Erfindung betrifft ein Verfahren zum Nachweis der Abstammung und/oder zur Identifizierung von Tieren oder biologischem Material von Tieren und Organismen, welches die folgenden Schritte umfaßt: Speichern von Identifikationsdaten in Form einer verschlüsselten Nachricht, welche in einer eindeutigen vorgegebenen Beziehung zu einer genetischen Information steht, welche ein Tier oder das biologische Material eindeutig identifiziert, auf einem Datenträger, Überprüfen der Identifikationsdaten daraufhin, ob diese in der vorgegebenen Beziehung zu der genetischen Information stehen, sowie eine Chipkarte und ein Computersystem zur Verwendung bei diesem Verfahren und ein Verfahren zum Generieren der dem Tier zugeordneten Daten.</p> |  |  |  |

# **LEDIGLICH ZUR INFORMATION**

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

|    |                              |    |                                      |    |  |    |                                   |
|----|------------------------------|----|--------------------------------------|----|--|----|-----------------------------------|
| AL | Albanien                     | ES | Spanien                              | LS | Lesotho  | SI | Slowenien                         |
| AM | Armenien                     | FI | Finnland                             | LT | Litauen  | SK | Slowakei                          |
| AT | Österreich                   | FR | Frankreich                           | LU | Luxemburg  | SN | Senegal                           |
| AU | Australien                   | GA | Gabun                                | LV | Lettland   | SZ | Swasiland                         |
| AZ | Aserbaidshjan                | GB | Vereinigtes Königreich               | MC | Monaco   | TD | Tschad                            |
| BA | Bosnien-Herzegowina          | GE | Georgien                             | MD | Républik Moldau                                    | TG | Togo                              |
| BB | Barbados                     | GH | Ghana                                | MG | Madagaskar   | TJ | Tadschikistan                     |
| BE | Belgien                      | GN | Guinea                               | MK | Die ehemalige jugoslawische<br>Republik Mazedonien | TM | Turkmenistan                      |
| BF | Burkina Faso                 | GR | Griechenland                         | ML | Mali   | TR | Türkei                            |
| BG | Bulgarien                    | HU | Ungarn                               | MN | Mongolei   | TT | Trinidad und Tobago               |
| BJ | Benin                        | IE | Irland                               | MR | Mauretanien  | UA | Ukraine                           |
| BR | Brasilien                    | IL | Israel                               | MW | Malawi   | UG | Uganda                            |
| BY | Belarus                      | IS | Island                               | MX | Mexiko   | US | Vereinigte Staaten von<br>Amerika |
| CA | Kanada                       | IT | Italien                              | NE | Niger  | UZ | Usbekistan                        |
| CF | Zentralafrikanische Republik | JP | Japan                                | NL | Niederlande  | VN | Vietnam                           |
| CG | Kongo                        | KE | Kenia                                | NO | Norwegen   | YU | Jugoslawien                       |
| CH | Schweiz                      | KG | Kirgisistan                          | NZ | Neuseeland   | ZW | Zimbabwe                          |
| CI | Côte d'Ivoire                | KP | Demokratische Volksrepublik<br>Korea | PL | Polen  |    |                                   |
| CM | Kamerun                      | KR | Republik Korea                       | PT | Portugal   |    |                                   |
| CN | China                        | KZ | Kasachstan                           | RO | Rumänien   |    |                                   |
| CU | Kuba                         | LC | St. Lucia                            | RU | Russische Föderation                               |    |                                   |
| CZ | Tschechische Republik        | LI | Liechtenstein                        | SD | Sudan  |    |                                   |
| DE | Deutschland                  | LK | Sri Lanka                            | SE | Schweden   |    |                                   |
| DK | Dänemark                     | LR | Liberia                              | SG | Singapur   |    |                                   |
| EE | Estland                      |    |                                      |    |  |    |                                   |

Verfahren zum Nachweis der Abstammung und/oder zur Identifizierung von Tieren oder von biologischem Material

Die Erfindung betrifft ein Verfahren zum Nachweis der Abstammung und/oder zur Identifizierung von Tieren oder von biologischem Material. Dabei kann das biologische Material von Tieren oder von jeglichen Nukleinsäure als Erbsubstanz tragenden Organismen stammen.

Bei der Registrierung, beim Kauf oder bei der Zucht von Tieren kommt es häufig darauf an, die Identität eines Tieres eindeutig festzustellen, die Abstammung des Tieres nachzuweisen oder den Eigentümer zu ermitteln. Im Bereich der Tierzucht sind zum Nachweis der Abstammung und der Leistung von Zuchttieren sogenannte Zuchtbücher oder Zuchtregister bekannt, welche von anerkannten Züchtervereinigungen geführt werden. Darüber hinaus sind Tierpässe bekannt, welche bestimmte Daten jeweils eines Tieres enthalten. Zu diesen Daten zählen beispielsweise körperliche Merkmale, Ergebnisse von Bluttests, die Abstammung oder phänotypische Besonderheiten. Als nachteilig erweist sich hierbei, daß die Anzahl der Informationen gering, der Zugriff auf die Daten begrenzt und ihre Kontrolle schwierig ist. Insbesondere besteht bei allgemein zugänglichen Registern stets die Gefahr von Manipulationen durch die Benutzer.

Bei biologischem Material von Tieren oder Organismen, wie beispielsweise Zellproben oder Kulturen von Mikroorganismen besteht der Nachteil, daß ihre Identität häufig nicht nachgeprüft werden kann, da keine charakteristischen Daten vorhanden sind.

Die Erfindung löst diese Probleme durch ein Verfahren nach Anspruch 1 bzw. 32, einen Chipträger nach Anspruch 38 bzw. ein Computersystem nach Anspruch 41.

Die Erfindung kann vorsehen, daß die genetischen Informationen von mehreren Tieren oder von biologischem Material von mehreren Tieren oder Organismen bestimmt und auf einem Speichermedium als Referenzdatensätze abgespeichert werden und daß die genetische Information oder Teile der genetischen Information des zu identifizierenden Tieres oder des zu identifizierenden biologischen Materials mit einem Referenzdatensatz oder mehreren Referenzdatensätzen verglichen werden.

Die Erfindung kann auch vorsehen, daß in den Referenzdatensätzen zusätzlich Merkmale oder Eigenschaften der Tiere oder des biologischen Materials abgespeichert werden.

Die Erfindung kann auch vorsehen, daß die aus den genetischen Informationen herleitbaren Merkmale oder Eigenschaften ermittelt und im Referenzdatensatz abgespeichert werden.

Die Erfindung kann auch vorsehen, daß in den Referenzdatensätzen photographische Aufnahmen der Tiere abgespeichert werden.

Die Erfindung kann auch vorsehen, daß es sich bei dem biologischen Material um Embryonen, Samen- oder Eizellen von Tieren handelt.

Die Erfindung kann auch vorsehen, daß es sich bei dem biologischen Material um Blut- oder Gewebeproben von Tieren oder um Zellkulturzellen oder um Mikroorganismen handelt.

Die Erfindung kann auch vorsehen, daß die Referenzdatensätze bei einer zentralen Stelle abgespeichert werden.

Die Erfindung kann auch vorsehen, daß die Referenzdatensätze bei der zentralen Stelle verschlüsselt werden.

Die Erfindung kann auch vorsehen, daß als Schlüssel die jeweilige genetische Information verwendet wird. Die jeweilige genetische Information kann Teil des Schlüssels sein. Es kann auch vorgesehen sein, daß die jeweilige genetische Information Bestandteil eines elektronischen Zertifikates ist, welches den Schlüssel einem individuellen Tier, das durch die besagte genetische Information eindeutig spezifiziert ist, eindeutig zuweist und von einer Zertifizie-

rungsstelle ausgestellt ist. Die Form eines solchen Zertifikates kann sich weitgehend an der Form eines Zertifikates orientieren, das zur Authentifizierung eines öffentlichen Schlüssels im Rahmen des Gesetzes zur digitalen Signatur ausgestellt wird. Es enthält zumindest die besagte genetische Information, welche eine eindeutige Zuordnung zu einem individuellen Tier zuläßt, den dieser Information bzw. diesem individuellen Tier zugewiesenen Schlüssel, bei einer asymmetrischen Verschlüsselung den öffentlichen Schlüssel, sowie eine digitale Unterschrift der Zertifizierungsstelle, welche beglaubigt, daß die Zuordnung tatsächlich authentisch ist.

Die Erfindung kann auch vorsehen, daß zum Abrufen eines Referenzdatensatzes eine Chipkarte verwendet wird.

Die Erfindung kann auch vorsehen, daß zum Abrufen eines Referenzdatensatzes ein Paßwort oder eine andere Information zum Identifizieren eines Benutzers eingegeben wird.

Die Erfindung kann auch vorsehen, daß anhand der genetischen Informationen und gegebenenfalls weiteren Informationen der Referenzdatensätze Paarungsvorschläge für Züchtungen ermittelt werden.

Die Erfindung kann auch vorsehen, daß das die Referenzdaten enthaltende Speichermedium in eine vom Tier getragene Erkennungsmarke integriert wird.

Die Erfindung kann auch vorsehen, daß die genetische Information der Referenzdatensätze durch eine mit dem Speichermedium verbundene Ausgabevorrichtung in Form eines Säulendiagramms angezeigt wird.

Gemäß einem weiteren Aspekt der Erfindung stellt diese ein Verfahren zum Nachweis der Abstammung und/oder zur Identifizierung von Tieren oder von biologischem Material von Tieren und Organismen zur Verfügung, welches die folgenden Schritte umfaßt:

- Speichern von Identifikationsdaten in Form einer verschlüsselten Nachricht, welche in einer eindeutigen vorgegebenen Beziehung zu einer genetischen Information steht, welche ein Tier oder das biologische Material eindeutig identifiziert, auf einem Datenträger,

- Überprüfen der Identifikationsdaten daraufhin, ob diese in der vorgegebenen Beziehung zu der genetischen Information stehen.

Die verschlüsselte Nachricht, welche die Identifikationsdaten bilden, kann der genetischen Information dadurch zugeordnet sein, daß eine Nachricht, vorzugsweise bestimmten Inhaltes, mit einem Code verschlüsselt ist, welcher der genetischen Information und damit dem individuellen Tier eindeutig zugeordnet ist, und/oder dadurch, daß die verschlüsselte Nachricht eine Information enthält, welche in einer eindeutigen vorgegebenen Beziehung zu der besagten genetischen Information steht und im einfachsten Fall diese Information selbst sein kann. Beide Möglichkeiten können kombiniert werden. Im ersten Fall kann die vorgegebene Beziehung dadurch überprüft werden, daß die Nachricht mit dem dem Tier individuell zugeordneten Schlüssel entschlüsselt wird. Ist eine erfolgreiche Entschlüsselung möglich, ist nachgewiesen, daß die Identifikationsdaten tatsächlich der besagten genetischen Information zugeordnet sind. Im zweiten Fall wird mit einem Schlüssel, der bei einer vertrauenswürdigen Stelle hinterlegt ist bzw. nur vertrauenswürdigen Benutzern zugänglich gemacht wird, die verschlüsselte Nachricht entschlüsselt und anhand des Inhalts der Nachricht überprüft, ob diese Daten bzw. diese Nachricht zu einem bestimmten Tier gehört. Werden beide Verfahren kombiniert, erfolgt eine Verifizierung der Zuordnung zu der genetischen Information bzw. zu dem Tier in doppelter Weise, zum einen durch die erfolgreiche Entschlüsselung und zum anderen durch den Inhalt der entschlüsselten Nachricht.

Das erfindungsgemäße Verfahren kann insbesondere die folgenden Schritte umfassen:

- Speichern von genetischen Informationen auf einem Datenträger, welcher das Tier bzw. das Material eindeutig identifizieren, in Verbindung mit Identifikationsdaten, die eine verschlüsselte Nachricht enthalten, die in einer eindeutigen Beziehung zu den genetischen Informationen steht,
- Aufrufen der Identifikationsdaten durch eine verschlüsselte Nachricht, die in eindeutiger Beziehung zu den genetischen Informationen steht,
- Überprüfen der Identifikationsdaten dahingehend, ob die mit der Nachricht übermittelten genetischen Informationen den gespeicherten genetischen Informationen entsprechen bzw. die gespeicherte verschlüsselte Nachricht der gesendeten verschlüsselten Nachricht entspricht,

- Ausgabe der genetischen Informationen, wenn eine Übereinstimmung festgestellt wurde und damit das Tier bzw. das Material eindeutig identifiziert wurde.

Die Erfindung kann auch vorsehen, daß die genetischen Informationen von einem oder mehreren Tieren oder von biologischem Material von einem oder mehreren Tieren oder Organismen bestimmt und auf einem Speichermedium als Referenzdatensätze abgespeichert werden.

Die Referenzdatensätze enthalten die Identifikationsdaten sowie gegebenenfalls weitere Daten betreffend das jeweilige Tier und bilden somit gewissermaßen ein elektronisches Registerblatt, auf dem die das Tier betreffenden Daten eingetragen sind und das durch die Identifikationsdaten eindeutig dem individuellen Tier zugeordnet ist.

Die Erfindung kann auch vorsehen, daß auf dem Datenträger den Identifikationsdaten zugeordnet weitere Daten betreffend das zu identifizierende Tier bzw. das zu identifizierende biologische Material gespeichert sind. Dabei kann insbesondere vorgesehen sein, daß die verschlüsselten Identifikationsdaten einen Zeiger oder eine anderweitige Information über den Speicherort der besagten weiteren Daten enthalten, so daß diese Information, d. h. die Zuordnung eines bestimmten Speicherbereichs zu einem bestimmten Tier, ohne Kenntnis des Schlüssels nicht verändert werden kann. Ein Versuch, einem bestimmten Tier einen anderen Datensatz zuzuordnen, würde daher beim Entschlüsseln der Identifikationsdaten auffallen, da sich entweder kein vernünftiger Klartext ergibt oder die entschlüsselte Information über den Speicherort bzw. den Zeiger zu den gespeicherten Daten betreffend das Tier nicht richtig ist. Die Erfindung kann auch vorsehen, daß die Identifikationsdaten eine verschlüsselte Nachricht enthalten, welche mit einem dem individuellen Tier oder Material eindeutig zugeordneten Code verschlüsselt ist.

Die Erfindung kann auch vorsehen, daß die verschlüsselte Nachricht den Wert einer Einwegfunktion (Hash) enthält, der sich ergibt, wenn diese Einwegfunktion auf weitere auf dem Datenträger gespeicherte Daten betreffend das zu identifizierende Tier bzw. das zu identifizierende biologische Material angewendet wird.

Die Erfindung kann auch vorsehen, daß eine verschlüsselte Nachricht eine das Tier bzw. das Material eindeutig identifizierende genetische Information umfaßt.

Die Erfindung kann auch vorsehen, daß die Identifikationsdaten verschlüsselte Daten betreffend den Speicherort und/oder den Inhalt von weiteren Daten betreffend das den Identifikationsdaten zugeordnete Tier umfassen.

Die Erfindung kann auch vorsehen, daß die Identifikationsdaten eine Nachricht umfassen, die mit einem Code verschlüsselt wird, welcher auf der Grundlage einer Ziffernfolge in einer vorbestimmten eindeutigen Weise generiert ist, welche einer genetischen Information, welche das Tier bzw. das Material eindeutig identifiziert, eindeutig zugeordnet ist.

Die Erfindung kann auch vorsehen, daß die Ziffernfolge zumindest einen Teil des Codes bildet.

Die Erfindung kann auch vorsehen, daß der Schlüssel ein symmetrischer Schlüssel ist.

Die Erfindung kann auch vorsehen, daß die Information auf der Grundlage eines asymmetrischen Schlüsselpaares verschlüsselt wird, wobei zumindest ein Teil des öffentlichen Schlüssels in einer vorgegebenen Beziehung zu der das Tier bzw. das Material identifizierenden genetischen Information steht.

Die Erfindung kann auch vorsehen, daß der öffentliche Schlüssel aus einem für das Tier bzw. das Material spezifischen Anteil und einem benutzerspezifischen Anteil besteht.

Die Erfindung kann auch vorsehen, daß die Identifikationsdaten zusätzlich mit einem benutzerspezifischen Schlüssel verschlüsselt werden.

Die Erfindung kann auch vorsehen, daß zumindest ein Teil der Daten auf dem Datenträger, welche den Identifikationsdaten zugeordnet sind, mit einem Code verschlüsselt sind, der verschieden von dem Code ist, mit welchem die Identifikationsdaten verschlüsselt sind.

Die Erfindung kann auch vorsehen, daß der Schlüssel zum Entschlüsseln der in den Identifikationsdaten enthaltenen Nachricht auf einem Träger eines Chips zum Kommunizieren mit

einer Datenverarbeitungsanlage über eine Schnittstelle, z. B. ein Lesegerät, insbesondere auf einer Chipkarte, gespeichert ist.

Unter einem Chip im Sinne dieser Anmeldung soll allgemein jeder elektronische oder optische Baustein verstanden werden, welcher zumindest eine Speicherfunktion hat und gegebenenfalls auch logische Funktionen ausführen kann und eine Schnittstelle zur Kommunikation mit einem Rechnersystem, z. B. über ein Lesegerät oder über eine optische Schnittstelle, aufweist. Insbesondere sollen hiervon auch holographische Speichereinheiten mit umfaßt werden. In dem Chip können außer den Identifikationsdaten sowie gegebenenfalls einem elektronischen Zertifikat einer Zertifizierungsstelle auch weitere das Tier betreffende Daten gespeichert sein, z. B. Impfdaten, Abstammungsdaten etc., so daß der Chip oder ein Träger, auf dem dieser Chip installiert ist, z. B. eine Chipkarte, als Tierausweis fungiert, auf dem alle für das Tier relevanten Daten gespeichert sind.

Die Erfindung kann auch vorsehen, daß der Chip eine Einrichtung zum Entschlüsseln von Nachrichten aufweist.

Die Erfindung kann auch vorsehen, daß der die Nachricht der Identifikationsdaten codierende Schlüssel ein asymmetrischer Schlüssel ist, der zugehörige private Schlüssel auf dem Chip gespeichert ist und der Chip eine Einrichtung zum Verschlüsseln von Nachrichten mit dem privaten Schlüssel aufweist.

Die Erfindung kann auch vorsehen, daß der Chip eine Schnittstelle zum Eingeben von digitalisierter genetischer Information und eine Einrichtung zum Überprüfen der Zuordnung des gespeicherten Codes zu einer eingegebenen digitalisierten genetischen Information enthält.

Die Erfindung kann auch vorsehen, daß die Vergleichseinrichtung die eingegebene digitalisierte genetische Information mit einem abgespeicherten Wert für diese Information vergleicht und ein Ausgangssignal abgibt, welches anzeigt, ob eine Übereinstimmung vorliegt oder nicht.

Die Erfindung kann auch vorsehen, daß die Vergleichseinrichtung auf der Grundlage der eingegebenen digitalisierten genetischen Information und einer abgespeicherten Zuordnung einer

digitalisierten genetischen Information, welche das Tier bzw. das Material eindeutig identifiziert, zu dem abgespeicherten Schlüssel einen der eingegebenen Information zugeordneten Schlüssel bestimmt, den so bestimmten Schlüssel mit dem abgespeicherten Schlüssel vergleicht und ein Ausgangssignal abgibt, welches anzeigt, ob der aufgrund der eingegebenen Information bestimmte Schlüssel mit dem abgespeicherten Schlüssel übereinstimmt oder nicht.

Die Erfindung kann auch vorsehen, daß in dem Chip einen oder mehrere Benutzer identifizierende Informationen gespeichert sind und die Entschlüsselungs- bzw. Verschlüsselungseinrichtung nur dann aktiviert wird, wenn über eine Eingabeeinrichtung eine für einen Benutzer als Identifizierung gespeicherte Information eingegeben wird. Die betreffende Information kann z. B. ein Paßwort sein, aber auch z. B. ein Fingerabdruck, das Abbild der Netzhaut, ein Sprachmuster zur Spracherkennung oder dgl.

Die Erfindung kann auch vorsehen, daß der Code zum Entschlüsseln von codierter Information, die in den Identifikationsdaten enthalten ist, in einem zentralen Rechner gespeichert ist.

Die Erfindung kann auch vorsehen, daß der Rechner aufgrund einer eingegebenen oder vorgegebenen genetischen Information den zugehörigen Schlüssel bestimmt und diesen Schlüssel auf die Identifikationsdaten anwendet.

Der Rechner kann dabei als reiner Entschlüsselungsserver fungieren, d. h. die jeweiligen Daten sind anderweitig, in der Regel dezentral, gespeichert, wobei an den jeweiligen Speicherorten der zur Entschlüsselung notwendige Schlüssel nicht vorhanden ist und nur auf dem besagten zentralen Rechner eine Entschlüsselung stattfindet, wobei der Zentralrechner die verschlüsselten Daten empfängt und die entschlüsselten Daten zurücksendet. Es kann auch vorgesehen sein, daß die entsprechenden tierbezogenen Daten ebenfalls auf dem zentralen Rechner gespeichert sind. In diesem Fall dient der Schlüssel, welcher die Identifikationsdaten entschlüsselt, im wesentlichen zum Nachweis, daß die Zuordnung der Daten in dem Rechner zu einem bestimmten Tier bzw., wenn eine Einwegfunktion verwendet wird oder die gesamten Daten verschlüsselt sind, daß die Daten insgesamt nicht manipuliert wurden. Dagegen ist die Kommunikation zwischen dem Rechner und dem Benutzer bei dieser Variante nicht gegen

Manipulationen gesichert oder wird durch ein standardmäßiges Verfahren zum Herstellen einer sicheren Verbindung zwischen einem Server und einem Benutzer abgesichert.

Die Erfindung kann auch vorsehen, daß der zentrale Rechner nach der Entschlüsselung überprüft, ob vorgegebene Zeichenfolgen in dem entschlüsselten Klartext vorhanden sind und ein entsprechendes Ausgangssignal an einen Benutzer abgibt.

Die Erfindung kann auch vorsehen, daß die auf einem von dem zentralen Rechner getrennten Datenträger gespeicherte tierbezogene Information sowie gegebenenfalls eine vorbestimmte, das Tier bzw. das Material eindeutig identifizierende genetische Information zu dem zentralen Rechner übermittelt wird, wo sie entschlüsselt wird.

Die Erfindung kann auch vorsehen, daß der Datenträger mit den auf das Tier bzw. das Material bezogenen Daten auf einem zentralen Rechner installiert ist.

Die Erfindung kann auch vorsehen, daß zumindest ein Teil der Daten zugriffsgeschützt ist und die Zugriffsberechtigung für verschiedene Benutzer des zentralen Rechners verschieden ist.

Die Erfindung kann auch vorsehen, daß für einen Teil der Benutzer ein Zugriff auf zumindest einen Teil der gespeicherten Daten nur dann möglich ist, wenn gleichzeitig ein vorbestimmter weiterer Benutzer, z. B. der Tierbesitzer, bei dem zentralen Rechner angemeldet ist.

Die Erfindung kann auch vorsehen, daß ein Zugriff auf zumindest einen Teil der gespeicherten Daten nur dann möglich ist, wenn der Rechner anhand der auf einem Chip, insbesondere auf einer Chipkarte, gespeicherten Daten die Zugriffsberechtigung überprüft hat. Dies kann insbesondere auch für den zweiten Benutzer gelten, der gemäß der vorangehend genannten Ausführungsform angemeldet sein muß.

Die Erfindung kann auch vorsehen, daß der Rechner so eingerichtet ist, daß ein Schreiben von Benutzern in die abgespeicherten, auf das Tier bzw. das Material bezogenen Daten nur zusammen mit einer digitalen Signatur des Benutzers möglich ist.

Die Erfindung kann auch vorsehen, daß ein tierspezifisches Paar von asymmetrischen Schlüsseln zum Austausch eines Sitzungsschlüssels für die Kommunikation eines Benutzers mit dem zentralen Rechner verwendet wird.

Die Erfindung stellt auch ein Verfahren zum Generieren von Daten zur Verfügung, welche zu einem individuellen Tier nachprüfbar in einer eindeutigen Beziehung stehen, welches umfaßt:

- Erzeugen von Identifikationsdaten in Form einer verschlüsselten Nachricht, welche in einer eindeutigen vorgegebenen Beziehung zu einer genetischen Information steht, welche ein Tier oder das biologische Material eindeutig identifiziert.
- Speichern der Identifikationsdaten auf einem Datenträger.

Die Erfindung kann auch vorsehen, daß die Identifikationsdaten eine verschlüsselte Nachricht enthalten, welche mit einem dem individuellen Tier eindeutig zugeordneten Schlüssel verschlüsselt ist.

Die Erfindung kann auch vorsehen, daß die verschlüsselte Nachricht den Wert einer Einwegfunktion (Hash) enthält, der sich ergibt, wenn diese Einwegfunktion auf weitere auf dem Datenträger gespeicherte Daten betreffend das zu identifizierende Tier bzw. das zu identifizierende biologische Material angewendet wird.

Die Erfindung kann auch vorsehen, daß die Identifikationsdaten eine Nachricht umfassen, die mit einem Code verschlüsselt ist, welcher auf der Grundlage einer Ziffernfolge in einer vorbestimmten eindeutigen Weise generiert ist, welche einer genetischen Information, welche das Tier bzw. das Material eindeutig identifiziert, eindeutig zugeordnet ist.

Die Erfindung kann auch vorsehen, daß der Schlüssel ein symmetrischer Schlüssel ist.

Die Erfindung kann auch vorsehen, daß die Information auf der Grundlage eines asymmetrischen Schlüsselpaares verschlüsselt ist, wobei zumindest ein Teil des öffentlichen Schlüssels in einer vorgegebenen Beziehung zu der genetischen Information steht.

Die Erfindung stellt auch einen Chipträger zur Identifizierung von Tieren zur Verfügung, der zur Kommunikation zwischen einem Chip auf dem Chipträger und einem Rechner über eine

Schnittstelle, z. B. ein Lesegerät, eingerichtet ist, insbesondere eine Chipkarte, dadurch gekennzeichnet, daß auf dem Chip ein Schlüssel gespeichert ist, der zu einer für das individuelle Tier spezifischen genetischen Information in einer eindeutigen vorgegebenen Beziehung steht.

Die Erfindung kann auch vorsehen, daß der Chip einen Prozessor zum Entschlüsseln von Nachrichten mit dem gespeicherten Schlüssel aufweist.

Die Erfindung kann auch vorsehen, daß der Chip eine Schnittstelle zum Eingeben von digitalisierter genetischer Information und eine Vergleichseinrichtung zum Überprüfen der Zuordnung des gespeicherten Codes zu einer eingegebenen digitalisierten genetischen Information enthält.

Die Erfindung stellt auch ein Computersystem zur Durchführung eines Verfahrens wie vorangehend beschrieben zur Verfügung, das einen zentralen Rechner aufweist, welcher einen Datenträger aufweist, auf dem Identifikationsdaten gespeichert sind, die in einer eindeutigen vorgegebenen Beziehung zu einer genetischen Information stehen, welche ein Tier oder das biologische Material eindeutig identifiziert.

Das erfindungsgemäße Verfahren hat den Vorteil, daß zur Identifizierung und zum Nachweis der Abstammung die genetischen Informationen der Tiere oder des biologischen Materials herangezogen werden. Die genetischen Informationen werden beispielsweise aus einer Blut- oder Gewebeprobe der Tiere oder aus deren Ei- oder Samenzellen nach bekannten Methoden bestimmt. Als Gewebeprobe ist zum Beispiel eine Haarwurzel ausreichend. Träger der genetischen Information sind die Ribonukleinsäuren (RNS), welche die stoffliche Substanz der Gene darstellen und die Fähigkeit zur identischen Verdopplung besitzen. Die genetische Information kann auf verschiedene Arten zusammengefaßt oder auch standardisiert werden. Zur Darlegung bestimmter Eigenschaften können die dafür kodierten Gene oder genetische Marker verwendet werden. Um den Zugriff auf die genetische Information zu gewährleisten, wird diese in Form von Referenzdatensätzen auf einem Speichermedium abgespeichert. Um die Identität eines Tieres festzustellen oder die Abstammung von Tieren oder von biologischem Material nachzuweisen oder zu überprüfen, werden die Referenzdatensätze vom Speichermedium abgerufen und mit bereits vorhandenen Daten verglichen. Bevor ein Benutzer auf den

Referenzdatensatz zugreifen kann, muß er zunächst seine Berechtigung nachweisen. Dies kann beispielsweise durch Eingabe eines Paßwortes, eines Namens oder einer PIN erfolgen. Darüber hinaus kann die Berechtigung auch auf einer Chipkarte, beispielsweise einer Smart-Card, abgespeichert sein. Der Benutzer kann jeweils nur denjenigen Referenzdatensatz abrufen, zu dem er die Berechtigung nachweisen kann. Alle anderen auf dem Speichermedium abgelegten Referenzdatensätze sind für ihn nicht zugänglich. Bei diesem Benutzer kann es sich beispielsweise um den Besitzer eines Tieres handeln. Er kann seine Berechtigung auch an Dritte weitergeben. Auf diese Weise kann beispielsweise der Käufer eines Tieres schnell und einfach nachprüfen, ob die von dem Verkäufer angegebenen Daten zu dem zum Kauf angebotenen Tier gehören. In diesem Fall wird die Berechtigung an den Kaufinteressenten zeitlich begrenzt. Werden vermißte Tiere wieder aufgefunden, so kann nachgeprüft werden, ob es sich um das gesuchte Tier handelt. In beiden Fällen können dem Tier Zellproben entnommen werden, um eine gewisse Anzahl genetischer Informationen daraus zu ermitteln. Aus dem Vergleich zwischen den ermittelten Informationen und den Referenzdatensätzen ergibt sich die Identität des Tieres. Mit Hilfe der genetischen Informationen kann außerdem die Abstammung der Tiere überprüft werden. Für die Tierzucht werden häufig den Tieren Samenzellen oder Eizellen entnommen und diese entsprechend aufbewahrt. Die in geeigneten Behältnissen gelagerten Geschlechtszellen stehen im Bedarfsfall zur Verfügung. Beim Kauf derartiger Geschlechtszellen kann der Käufer durch Entnahme einer Probe und dem Vergleich zwischen den aus der Probe ermittelten Daten und einem Referenzdatensatz die Abstammung der Geschlechtszellen ermitteln. Auf diese Weise können außerdem für ein optimales Zuchtergebnis geeignete Paarungsvorschläge ermittelt werden.

Die Gefahr von Manipulationen der Referenzdaten besteht bei diesem Verfahren nicht, da ein Abrufen der Daten nur durch Berechtigte möglich ist. Die Veränderung der Referenzdaten kann außerdem nur einer zentralen Stelle gestattet sein, so daß selbst Berechtigte die Daten nicht verändern können. Der Inhalt des Referenzdatensatzes liefert einen genetischen Fingerabdruck des betreffenden Tieres, des Organismus oder des biologischen Materials. Dieser erlaubt eine eindeutige Identifizierung und ist von jedem beliebigen Labor nachprüfbar.

Biologisches Material von Tieren oder Organismen kann zur Aufbewahrung oder Handhabung in geeigneten Behältnissen gelagert sein, welche mit einem Speichermedium für die genetischen Informationen des biologischen Materials versehen sind. Zur Überprüfung des

Inhalts werden die aus einer Probe des biologischen Materials ermittelten genetischen Informationen mit den gespeicherten Daten verglichen.

Nach einer vorteilhaften Ausgestaltung der Erfindung werden in den Referenzdatensätzen zusätzlich Merkmale oder Eigenschaften der Tiere oder des biologischen Materials abgespeichert. Auf diese Weise entsteht eine direkte Verbindung zwischen den allgemeinen Merkmalen und Eigenschaften des betreffenden Tieres und der in den Referenzdaten enthaltenen genetischen Information, welche das Tier eindeutig identifiziert („genetischer Fingerabdruck“). Dabei kann es sich z. B. um besondere Fähigkeiten des Tieres, um den Besitzer, um Vorfahren und Nachkommen, um Preise oder Auszeichnungen, um Wertangaben, um Angaben über allgemeine und besondere Fähigkeiten, um Ausbildungen, um Erbkrankheiten, sonstige Krankheiten, Impfungen oder tierärztliche Betreuungsdaten handeln. Der Einblick in den Referenzdatensatz erlaubt damit nicht nur die Kenntnisnahme der abstrakten genetischen Informationen, sondern ermöglicht außerdem das Abrufen charakteristischer Daten des Tieres oder des biologischen Materials. Auf diese Weise kann auch der Zusammenhang zwischen bestimmten genetischen Informationen und charakteristischen Merkmalen des Tieres oder des biologischen Materials untersucht, ausgewertet oder angegeben werden.

Nach einer weiteren vorteilhaften Ausgestaltung der Erfindung, werden die aus den genetischen Informationen herleitbaren Merkmale oder Eigenschaften ermittelt und in dem Referenzdatensatz abgespeichert. Bei den charakteristischen Merkmalen oder Eigenschaften des Tieres kann es sich nicht nur um solche handeln, die bei einer Untersuchung oder bei einer Beobachtung über einen längeren Zeitraum ermittelt wurden oder auf Erfahrungswerten beruhen, sondern auch um solche, die sich unmittelbar aus den genetischen Informationen ergeben. Sofern die genetischen Informationen in Form eines Referenzdatensatzes auf einem Speichermedium vorliegen, können bereits bekannte Gesetzmäßigkeiten oder auch neueste Erkenntnisse ausgenutzt werden, um auf schnelle und einfache Art und Weise die aus den genetischen Informationen resultierenden Merkmale anzugeben.

Nach einer weiteren vorteilhaften Ausgestaltung der Erfindung werden in den Referenzdatensätzen photographische Aufnahmen abgespeichert. Dies können insbesondere normale photographische Aufnahmen sein, welche das Aussehen des Tieres insgesamt zeigen, aber auch Ergebnisse bildgebender diagnostischer Verfahren (z. B. einer Ultraschalluntersuchung, einer

Röntgenuntersuchung, einer Endoskopie, einer Computertomographie), mit denen der körperliche Zustand des Tieres dokumentiert wird.

Nach einer weiteren vorteilhaften Ausgestaltung der Erfindung handelt es sich bei dem biologischen Material um Embryonen, Samen- oder Eizellen von Tieren. Diese werden, nachdem sie dem betreffenden Tier abgenommen worden sind, in geeignete Behältnisse abgefüllt und gekühlt gelagert. An den Behältnissen können Beschriftungen oder elektronische Datenträger, z. B. Mikrochips oder sogenannte Smart Labels, vorgesehen sein, welchen die für den Inhalt des Behälters wesentlichen Daten enthalten. Bei den Smart Labels handelt es sich um sehr dünne Speichereinheiten mit einer Ein- und Ausgabeschnittstelle, die wie ein Transponder wirkt. Diese Smart Labels können die Dicke eines Blattes Papier haben und damit anstelle von Papieretiketten als „elektronische Etiketten“ verwendet werden.

Der Zugriff auf die Referenzdaten ermöglicht ein Überprüfen der auf den Behältern angegebenen Daten insbesondere dann, wenn von den Samen- oder Eizellen eine Probe entnommen und daraus die genetische Information bestimmt wird.

Nach einer weiteren vorteilhaften Ausgestaltung der Erfindung handelt es sich bei den biologischen Material um Blut- oder Gewebeproben von Tieren, um Zellkulturzellen oder um Mikroorganismen. Diese können beispielsweise zu Prüf- oder Versuchszwecken gelagert werden. Eine Überprüfung der Probe ist in diesem Fall jederzeit möglich.

Nach einer weiteren vorteilhaften Ausgestaltung der Erfindung werden die Referenzdatensätze bei einer zentralen Stelle abgespeichert. Diese zentrale Stelle verwaltet und überwacht die Daten, so daß diese nicht durch Dritte manipuliert oder verfälscht werden können. Berechtigte können bei der zentralen Stelle auf die abgespeicherten Daten zugreifen. Die zentrale Stelle kann auch die betreffenden Berechtigungen vergeben.

Nach einer weiteren vorteilhaften Ausgestaltung der Erfindung werden die Referenzdatensätze bei der zentralen Stelle verschlüsselt. Dies erschwert den Zugriff von Unberechtigten auf die Daten und verhindert eine entsprechende Manipulation der Daten. So kann beispielsweise ein öffentlicher Schlüssel (public key) und ein privater Schlüssel (private key) zum Ver- und

Entschlüsseln der Daten vorgesehen sein. Durch das Abrufen der Referenzdaten gibt der Benutzer seine Unterschrift zum Inhalt des Datensatzes, vergleichbar einer digitalen Signatur.

Nach einer weiteren vorteilhaften Ausgestaltung der Erfindung wird als Schlüssel die jeweilige genetische Information verwendet oder dem Schlüssel die jeweilige genetischen Information zugrundegelegt. So kann beispielsweise die aus der Probe des Tieres ermittelte Basenzahl mit einer lediglich bei der zentralen Stelle bekannten Kontrollzahl verrechnet und als privater Schlüssel verwendet werden.

Nach einer weiteren vorteilhaften Ausgestaltung der Erfindung wird die Berechtigung zum Abrufen eines Referenzdatensatzes auf einer Chipkarte, insbesondere auf einer SmartCard, abgespeichert. Um den Referenzdatensatz abzurufen muß die Chipkarte in ein hierfür vorgesehenes Lesegerät eingeführt werden. Erst wenn die Berechtigung nachgeprüft und erkannt wurde, erfolgt die Ausgabe der Referenzdaten. Der Nutzer der Karte erhält eine geeignete Software, mit Hilfe der er an seinem Computer auf die Referenzdaten zugreifen kann. Bei einem Datennetz besteht die Möglichkeit, Online auf die Referenzdaten zuzugreifen. Hierzu ist eine geeignete Datenverbindung zwischen der zentralen Stelle und dem Nutzer notwendig. Anstelle einer Chipkarte kann auch ein anderer Träger eines isolierten Chips mit einer Schnittstelle zur Kommunikation mit einem Rechner vorgesehen sein, z. B. in Form eines Armbandes, eines Schlüsselbundes oder eines anderen Gegenstandes, den der Benutzer am Körper tragen kann, wobei die Schnittstelle nicht notwendig elektronisch sein muß, sondern gegebenenfalls auch optisch funktionieren kann. Unter dem Begriff „Chip“ im Rahmen dieser Anmeldung sollen nicht nur elektronische Halbleiterbausteine mit einer Speicherfunktion und einem eingebauten Mikroprozessor verstanden werden, sondern auch Speicherchips mit einer reinen Speicherfunktion oder andere, ähnlich dimensionierte Speicher – und/oder Logikeinheiten, beispielsweise holographische Speicher oder dergleichen. Dementsprechend ist auch mit einer „Chipkarte“ bzw. einem „Chipträger“ im Sinne dieser Anmeldung ein Träger bzw. eine Karte gemeint, welche einen Chip im Sinne dieser Anmeldung trägt. Der Chipträger hat im Regelfall ähnliche oder kleinere Abmessungen wie eine Chipkarte.

Nach einer weiteren vorteilhaften Ausgestaltung der Erfindung wird zum Nachweis der Berechtigung beim Abrufen eines Referenzdatensatzes ein Paßwort, ein Name oder eine PIN eingegeben.

Nach einer weiteren vorteilhaften Ausgestaltung der Erfindung werden an Hand der genetischen Informationen der Referenzdatensätze Paarungsvorschläge für Züchtungen ermittelt. Hierzu können aus den Referenzdatensätzen geeignete männliche und weibliche Tiere ausgewählt werden, um ein gewünschtes Zuchtergebnis zu erzielen. Die in Form von Referenzdatensätzen vorliegenden Daten erleichtern die Auswahl unter einer größeren Gesamtheit von Tieren.

Nach einer weiteren vorteilhaften Ausgestaltung der Erfindung wird das die Referenzdaten und gegebenenfalls Zugriffsberechtigungen enthaltende Speichermedium in eine vom Tier getragene Erkennungsmarke integriert. Dies erleichtert das Zuordnen der Tiere.

Nach einer weiteren vorteilhaften Ausgestaltung der Erfindung wird die genetische Information der Referenzdatensätze durch eine mit dem Speichermedium verbundene Ausgabevorrichtung in Form eines Säulendiagramms angezeigt. An Hand dieses Diagramms können die genetischen Informationen optisch schnell und einfach erfaßt und mit denjenigen anderen Tiere verglichen werden.

Nachfolgend werden einige Aspekte der Erfindung im einzelnen noch näher erläutert.

Ein Problem, welches häufig in Zusammenhang mit der Identifizierung von Tieren auftritt, ist, daß Unterlagen betreffend das Tier ausgetauscht werden und eine eindeutige Zuordnung des Inhalts der Unterlagen zu dem Tier nicht ohne weiteres möglich ist. Eine sichere Zuordnung des Schlüssels zu dem jeweiligen Tier bzw. zu berechtigten Personen ist ein großes Problem bei der Absicherung von identifizierenden Informationen gegenüber Fälschungen. Die Erfindung stellt insoweit ein Verfahren zur Verfügung, das eine sichere individualisierende Information (z. B. den genetischen Fingerabdruck) in die Erzeugung der Schlüssel integriert, sei es in die Schlüssel an sich oder in die Zertifikate, welche die von einer Zertifizierungsstelle zertifizierten Schlüssel bestimmten Personen bzw. Tieren zuordnen.

Gemäß einer bevorzugten Ausführungsform sieht die Erfindung zur Lösung dieses Problems vor, daß die tierbezogenen Daten auf dem Datenträger entweder selbst mit einem Schlüssel verschlüsselt sind, der in einer eindeutigen Beziehung zu einer das Tier eindeutig identifizie-

renden genetischen Information steht, oder daß eine verifizierende Information, welche weitere ursprünglich abgespeicherte Informationen, die nicht verschlüsselt sein müssen, nicht umkehrbar eindeutig identifiziert, mit einem solchem Code verschlüsselt ist. Derartige verifizierende Informationen lassen sich durch sogenannte Einwegfunktionen, auch Hash-Funktionen genannt, generieren. Wird nach dem Verschlüsseln die besagte weitere unverschlüsselte Information auf dem Datenträger manipuliert, läßt sich dies durch einen Vergleich zwischen dem codiert abgespeicherten Wert der Einwegfunktion und dem Wert feststellen, der sich ergibt, wenn die Einwegfunktion auf die tatsächlich auf dem Datenträger abgespeicherten Daten angewandt wird. Stimmen die beiden Werte nicht überein, sind die Daten verändert worden oder es wurde der falsche Schlüssel zum Entschlüsseln verwendet.

Eine genetische Information, welche ein Tier oder einen Organismus eindeutig identifiziert, läßt sich beispielsweise mit dem sogenannten Mikrosatellitenverfahren gewinnen. Bei diesem Verfahren wird ausgenutzt, daß in bestimmten Genomregionen eine bestimmte Basensequenz, z. B. CA, sich mit einer individuell unterschiedlichen Anzahl von Wiederholungen wiederholt. Diese Bereiche sind flankiert von stabilen Genomregionen, die als Zielsequenz für die Primerbindung bei einer Polymerase-Kettenreaktion (PCR) dienen. Wird die Anzahl dieser Wiederholungen in ausreichend vielen entsprechenden Genomregionen bestimmt, ist die Menge dieser Wiederholungen insgesamt spezifisch für das individuelle Tier bzw. den individuellen Organismus.

Legt man nun eine bestimmte Reihenfolge der Genomregionen, in denen diese Wiederholungen bestimmt werden, fest und ordnet Zahlen, die der Anzahl dieser Wiederholungen entsprechen, entsprechend dieser Reihenfolge an, ergibt sich daraus eine Ziffernfolge, die ebenfalls spezifisch für das konkrete Individuum ist.

Ein anderes Verfahren zur Darstellung individueller genetischer Information nutzt die Polymorphismen an einzelnen Nukleotidpositionen des Genoms. Das SNP (single nucleotide polymorphisms) -Verfahren liefert einen Datensatz, in dem für jede der untersuchten Genompositionen die Aussage 1 (= Ergebnis 1 z. B. entspricht dem Populationswert) oder 0 (= Ergebnis 2, z. B. abweichender Wert) erhalten wird. In ihrer Gesamtheit ergeben die Untersuchungsergebnisse einen binären Zahlenwert (z. B. 011100010100001111101010). Für eine sichere Individualisierung müssen ca. 40 Genompositionen untersucht werden. Gegenwärtig

sind weder beim Menschen noch bei anderen Organismen Standards definiert, welche die zu untersuchenden Positionen benennen. Für die Gewinnung der SNP-Informationen stehen verschiedene Verfahren zur Verfügung, welche zunehmend in Form von DNA-Chips automatisiert werden, wodurch ein hoher Probendurchsatz möglich wird. Beispiele der unterschiedlichen Ansätze sind das Verankern von Oligonukleotiden, die eine spezifische Position differenzieren, auf Chips. Eine andere Technik sieht vor, die polymorphen PCR-Produkte anhand ihres Molekulargewichtes zu unterscheiden. (Internationales Technologieforum 99, 23./24. Juni 1999, ICM Internationales Congress Center, Neue Messe München).

Die meisten Verschlüsselungsalgorithmen gehen von einer Zufallszahl aus, aufgrund derer dann der Schlüssel gebildet wird. Ersetzt man nun diese Zufallszahl durch eine in der vorangehenden Weise aus der genetischen Information gewonnene, für das Individuum spezifische Ziffernfolge, erhält man einen Verschlüsselungscode, der spezifisch für das betreffende Individuum ist. Allgemein kann zur Generierung des Schlüssels jede digitalisierte, vorzugsweise genetische Information verwendet werden, welche das Tier eindeutig identifiziert.

Erfindungsgemäß kann man dadurch, daß dem Tier eine Probe entnommen wird, die entsprechende genetische Information bestimmt wird und überprüft wird, ob der dieser Information entsprechende Schlüssel der Schlüssel zum Entschlüsseln der codierten Daten ist, überprüfen, ob das in Rede stehende Tier den abgespeicherten Daten entspricht. Läßt sich die verschlüsselte Information nicht entschlüsseln oder stimmt der gespeicherte Wert einer Einwegfunktion, da der verkehrte Schlüssel angewandt wurde, nicht mit den restlichen Daten, wie vorangehend beschrieben, überein, besteht der Verdacht auf eine Manipulation der Daten bzw. einen Austausch des Tieres. Auf diese Weise kann ausgeschlossen werden, daß das Tier, auf das sich die Daten beziehen, ausgetauscht worden ist.

Ein weiteres Problem besteht darin, daß die gespeicherten Daten auf dem Datenträger oder während des Transports über das Internet verfälscht werden können. Dieses Risiko läßt sich dadurch verringern, daß der Personenkreis, der Zugang zu dem Schlüssel bzw. zu der Zuordnung des Schlüssels zu der genetischen Information hat, beschränkt und kontrolliert wird. Man kann auch so vorgehen, daß der verschlüsselte Teil der Daten an eine vertrauenswürdige Zentralstelle zum Entschlüsseln geschickt wird, die das entschlüsselte Ergebnis zurückübermittelt, ohne den zur Entschlüsselung erforderlichen Schlüssel herauszugeben, und die gege-

benenfalls auch die Authentizität der Daten bzw. die Zuordnung des Tiers zu den gespeicherten Daten überprüft.

Dieses Verfahren ist jedoch umständlich und gibt keine Sicherheit, daß die zwischen der vertrauenswürdigen Stelle und einem Benutzer ausgetauschten Informationen unverfälscht bleiben. Weiterhin ist bei diesem Vorgehen wichtig, daß der Schlüssel selbst dem Besitzer des Tieres nach Möglichkeit nicht bekannt wird, da ansonsten die Gefahr von Fälschung der Daten mit dem richtigen Schlüssel besteht. Es wäre auch wünschenswert, daß ein Besitzer direkt anhand von genetischen Informationen überprüfen kann, ob das in Rede stehende Tier den abgespeicherten Daten entspricht.

Diese Probleme lassen sich dadurch umgehen, daß ein asymmetrisches Schlüsselpaar verwendet wird, wobei der öffentliche Schlüssel in einer vorbestimmten Beziehung zu der das Tier identifizierenden genetischen Information steht, die dem Benutzer bekannt sein kann oder von ihm direkt überprüft werden kann, während der private Schlüssel, mit dem die Daten verschlüsselt sind, nur derjenigen Person bzw. derjenigen Stelle bekannt oder bei ihr verfügbar ist, welche die Daten auf den Datenträger geschrieben hat bzw. hierzu berechtigt ist.

Asymmetrische Schlüssel sind in der Datentechnik allgemein bekannt und bilden unter anderem die Grundlage für die digitale Signatur. Hinsichtlich Einzelheiten betreffend die Verschlüsselung von Daten und anderen Aspekte der Datensicherheit, insbesondere auch Einweg- oder Hash-Funktionen, wird z. B. auf M. Raeppe, „Sicherheitskonzepte für das Internet“, Heidelberg 1998 oder auf RSA Laboratories, „Answers to Frequently Asked Questions About Today's Cryptography“, Version 3.0, verwiesen.

Nachfolgend wird ein Beispiel beschrieben, wie sich ein asymmetrischer RSA-Code auf der Grundlage einer genetischen Information erzeugen läßt.

Ein RSA-Code kann wie folgt erzeugt werden:

- man nehme zwei große Primzahlen  $p$  und  $q$ ,
- man bildet deren Produkt  $n = p \cdot q$ ,
- man wähle eine Zahl  $e$ , die kleiner als  $n$  und teilerfremd zu  $p - 1$  und  $q - 1$  ist,
- man finde eine Zahl  $d$  so, daß  $(e \cdot d) - 1$  durch  $(p - 1) \cdot (q - 1)$  teilbar ist.

Das Wertepaar  $(n, e)$  bildet den öffentlichen Schlüssel und das Paar  $(n, d)$  bildet den privaten Schlüssel. Die Faktoren  $p$  und  $q$  werden vernichtet oder mit dem privaten Schlüssel zusammen sicher aufbewahrt.

Zum Chiffrieren einer Nachricht  $m$  mit dem öffentlichen Schlüssel wird  $m$  modular entsprechend der Vorschrift  $c = m^e \bmod n$  potenziert. Zum Dechiffrieren wird die chiffrierte Nachricht  $c$  auf der Grundlage des privaten Schlüssels entsprechend der Vorschrift  $c^d \bmod n$  potenziert. Der RSA-Schlüssel ist gerade so konstruiert, daß sich dann genau wieder die ursprüngliche Nachricht  $m$  ergibt. Umgekehrt kann auch nach den gleichen Vorschriften zunächst mit dem privaten Schlüssel chiffriert und dann mit dem öffentlichen Schlüssel dechiffriert werden.

Zur Generierung eines tierspezifischen Schlüsselpaares kann man beispielsweise bei dem RSA-Algorithmus die aus der genetischen Information bestimmte Zahl gleich der Zahl  $e$  setzen, wobei nach Faktorisierung von  $e$  Primzahlen  $p$  und  $q$  gefunden werden, für die gilt, daß  $p - 1$  und  $q - 1$  teilerfremd zu  $e$  sind. Entsprechend dem RSA-Algorithmus wird dann die Zahl  $d$  bestimmt, so daß der öffentliche Schlüssel als einen Parameter die Zahl  $e$  enthält, die der vorangehend genannten genetischen Information entspricht. Wird nun eine Information in dem Datensatz, beispielsweise das Ergebnis einer Hash-Funktion, mit dem privaten Schlüssel, der nur dem Besitzer des Tiers, einer vertrauenswürdigen Stelle oder dergleichen zugänglich ist, verschlüsselt, so kann durch eine erfolgreiche Entschlüsselung mit dem öffentlichen Schlüssel nicht nur verifiziert werden, daß die gespeicherte Information sich tatsächlich auf das in Rede stehende Tier bezieht (was bei dem vorliegenden Beispiel durch einen Vergleich von  $e$  mit einer direkt von dem Tier gewonnenen genetischen Information möglich ist), sondern es kann auch, genau wie bei einer digitalen Signatur, verifiziert werden, wer die Verschlüsselung vorgenommen hat.

Man beachte in diesem Zusammenhang, daß der zweite Parameter des öffentlichen und privaten Schlüssels,  $n$ , bei dem vorangehend genannten Beispiel nicht eindeutig festgelegt ist. Dementsprechend ist es möglich, mehrere Schlüssel zu generieren, die in dem vorangehend genannten Sinn für das Tier spezifisch sind, aber zu verschiedenen Personen gehören. Dies

ermöglicht, daß verschiedene Personen, deren Authentizität unmittelbar überprüft werden kann, tierbezogene Daten auf den Datenträger schreiben können.

Eine weitere Möglichkeit, eine Authentifizierung der Person, welche Daten auf den Datenträger geschrieben hat, zu ermöglichen, besteht darin, daß die mit dem „tierspezifischen Code“ codierte Nachricht noch einmal durch einen für den jeweiligen Benutzer spezifischen Code verschlüsselt wird oder daß der betreffende Benutzer in herkömmlicher Weise einen von ihm generierten Text digital signiert, indem er z. B. von dem generierten Text den Wert einer Hash-Funktion berechnet und diesen Wert mit seinem privaten Schlüssel aus einem asymmetrischen Schlüsselpaar verschlüsselt, wobei dieser chiffrierte Wert dann dem Datensatz hinzugefügt wird.

Um die Verifizierung und die Sicherheit des verwendeten Schlüssels noch weiter zu erhöhen, kann vorgesehen sein, daß der zur Entschlüsselung nötige Schlüssel auf einer Chipkarte implementiert wird. Dabei kann entweder vorgesehen sein, daß ein zur Entschlüsselung verwendeter Computer auf den in der Chipkarte sicher gespeicherten Schlüssel zugreift und diesen bei der Entschlüsselung verwendet oder, was bevorzugt ist, daß die Chipkarte selbst einen Prozessor zum Entschlüsseln von Nachrichten enthält, so daß ein verschlüsselter Text in die Karte eingegeben wird und ein Klartext ausgegeben wird, während der gespeicherte Code selbst nicht nach außen gelangt. Die Chipkarte kann auch zum Aufbewahren des privaten Schlüssels eines Benutzers vorgesehen sein und vorzugsweise einen Prozessor zum Verschlüsseln von Nachrichten mit dem privaten Schlüssel aufweisen.

Die Zuordnung der Chipkarte zu einem bestimmten Tier kann auf verschiedene Weise hergestellt werden.

Die einfachste Möglichkeit ist, den öffentlichen Schlüssel, beispielsweise wie vorangehend erläutert, so zu wählen, daß eine für das Tier spezifische genetische Information Bestandteil des öffentlichen Schlüssels ist, beispielsweise so, daß diese Information den Parameter  $e$  bildet. Dabei kann der öffentliche Schlüssel im einfachsten Fall auf der Chipkarte aufgedruckt sein oder durch eine einfache Ausgabeoperation aus dem Speicher der Chipkarte abgerufen werden.

Wenn der öffentliche Schlüssel selbst nicht jedermann bekannt werden soll, kann auch vorgesehen sein, daß eine Zuordnungsvorschrift zwischen der genetischen Information und dem öffentlichen Schlüssel in dem Chip der Chipkarte gespeichert ist und die Chipkarte so eingerichtet ist, daß eine von dem konkreten Tier gewonnene digitalisierte genetische Information eingegeben werden kann. Ein Prozessor in der Chipkarte berechnet dann aus der eingegebenen digitalisierten Information entsprechend der Zuordnungsvorschrift den Schlüssel und vergleicht diesen mit dem abgespeicherten Schlüssel. Liegt Übereinstimmung vor, gibt der Prozessor aus, daß die eingegebene Information dem abgespeicherten Schlüssel entspricht, und macht eine Ausgabe, daß die Chipkarte nicht dem entsprechenden Tier entspricht, wenn keine Übereinstimmung zwischen dem gespeicherten Schlüssel und dem von dem Prozessor bestimmten Schlüssel vorliegt. Vorzugsweise enthält die Chipkarte weiterhin im Klartext abrufbare Informationen, nach welchem Verfahren die genetischen Informationen, die dem in der Chipkarte abgespeicherten Schlüssel zugrunde liegen, gewonnen wurden und nach welchem Verfahren die gewonnenen Informationen digitalisiert werden. Ein Benutzer, der über die entsprechenden genetischen Informationen betreffend das in Rede stehende Tier verfügt, benötigt daher keine Zertifizierungsstelle oder dergleichen, um festzustellen, ob ein bestimmter Code oder eine bestimmte Chipkarte tatsächlich einem bestimmten Tier zugeordnet sind. Er kann dies selbst anhand der von dem Tier gewonnenen genetischen Informationen und den in der Chipkarte gespeicherten Informationen feststellen. Damit entfallen auch alle Probleme, die durch die Kommunikation zwischen einem Benutzer und einer Zertifizierungsstelle bei der digitalen Signatur entstehen. Durch die physikalische Verbindung von Schlüsseln und das Tier identifizierende Daten auf der Chipkarte wird die Manipulation der Kommunikation bzw. der für den sicheren Datentransport erforderlichen Komponenten verhindert.

Mit dem vorangehend beschriebenen Verfahren läßt sich ein System zur Zertifizierung und Verifizierung von Tieren auf elektronischer Basis einrichten. Die das Tier betreffenden Daten, z. B. Geburtsdatum, Besitzerdaten, Impfdaten usw., werden auf einem zentralen Rechner bei einer Zertifizierungsstelle gespeichert, der in üblicher Weise für privilegierte Benutzer zugänglich ist und bei dem ggf. ein Teil der gespeicherten Daten öffentlich zugänglich ist. Die entsprechenden Daten sind entweder mit dem privaten Schlüssel eines tierspezifischen asymmetrischen Schlüsselpaares, also eines Codes, der in der vorangehend erwähnten Weise auf eine genetische Information eines bestimmten Tieres zurückgeht, verschlüsselt oder es ist jedem Datensatz, mit diesem tierspezifischen privaten Schlüssel verschlüsselt, der Wert einer

Einwegfunktion hinzugefügt, der sich ergibt, wenn diese Einwegfunktion auf den entsprechenden Datensatz angewendet wird. In beiden Fällen kann ein Benutzer, welcher die entsprechenden Daten liest oder über das Internet empfängt, verifizieren, daß diese unverfälscht sind und auf eine bestimmte Person zurückgehen.

Der Besitzer des Tieres erhält eine tierspezifische Chipkarte, auf welcher der tierspezifische asymmetrische Schlüssel abgespeichert ist, und zwar sowohl der private als auch der öffentliche Schlüssel. Die Chipkarte dient gleichzeitig als Tierausweiskarte, die ein Zertifikat der Zertifizierungsstelle enthält. Das Zertifikat enthält den Namen des Tieres, eine fortlaufende Seriennummer, den Namen des Ausstellers, den Namen des Antragstellers, den Namen derjenigen Stelle, welche die genetischen Informationen, die der Codierung zugrunde liegen („genetischer Fingerabdruck“), gewonnen hat, das Verfahren, wie diese Informationen gewonnen wurden, die genetischen Informationen selbst und eine Gültigkeitsdauer sowie gegebenenfalls die Angabe des öffentlichen Schlüssels und/oder des Verschlüsselungsverfahrens. Dieses Zertifikat ist im Klartext oder mit einem öffentlichen Schlüssel der Zertifizierungsstelle aus dem Chip auslesbar. Gegebenenfalls kann das Zertifikat auch auf der Chipkarte aufgedruckt sein.

Um Zugriff auf die bei der Zertifizierungsstelle gespeicherten Daten zu erhalten, werden die genetischen Informationen und der öffentliche Schlüssel über ein Lesegerät aus der Chipkarte ausgelesen und zu der Zertifizierungsstelle übermittelt. Anhand der genetischen Information bestimmt der Rechner der Zertifizierungsstelle, auf welches Tier bezogen Daten freigegeben werden sollen. Anhand des öffentlichen Schlüssels überprüft der Rechner, ob der angemeldete Benutzer zum Lesen der Daten berechtigt ist. Es können auch andere Daten übermittelt werden, z. B. eine Seriennummer, welche das betreffende Tier angibt, anstelle der genetischen Information. Zusätzliche oder alternative Zugangssperren, z. B. Paßwörter, können ebenfalls vorgesehen sein.

Der Besitzer erhält eine Zugriffsberechtigung für diejenigen Teile der in dem Zentralrechner abgespeicherten Daten, die besitzerbezogen sind, z. B. den Aufzuchtort, Ernährungsdaten oder dergleichen. Für andere Daten, beispielsweise auf das Geburtsdatum, den Herkunftsort oder dergleichen, erhält der Besitzer, obwohl er im Besitz des entsprechenden privaten Schlüssels ist, nur eine beschränkte Zugriffsberechtigung. In der Regel wird man ihm gestat-

ten, diese Daten zu lesen, aber nicht, sie zu ändern oder zu löschen. Die Zugriffsberechtigung kann in herkömmlicher Weise durch die Vergabe von Lese- und Schreibrechten bei dem zentralen Rechner und/oder ein konventionelles Paßwort eingerichtet werden. Andere Zugriffskontrollmechanismen, z. B. Spracherkennung oder die Verwendung von biologischen Merkmalen der betreffenden Person (Fingerabdruck, Irisabtastung etc.) können ebenfalls verwendet werden. Als weitere Möglichkeit der Zugangskontrolle kann auch vorgesehen sein, daß ein Zugriff auf Daten nur dann gestattet wird, wenn der Benutzer eine digitale Signatur hinterlegt, also eine Nachricht, die mit einem privaten Schlüssel codiert ist, der dem Benutzer von einer Zertifizierungsstelle zugewiesen ist, welche die Zertifizierungsstelle für die Tierdaten sein kann, aber auch eine Zertifizierungsstelle entsprechend dem Gesetz zur digitalen Signatur sein kann.

Es kann auch vorgesehen sein, daß mit einer einzigen Chipkarte (Mastercard) der Zugriff auf Daten betreffend mehrere Tiere, z. B. für Züchter oder Verbände, ermöglicht wird, wobei vorzugsweise diese Mastercard nur die jeweiligen öffentlichen Schlüssel enthält, nicht jedoch die privaten Schlüssel, so daß der Inhaber dieser Mastercard zwar sämtliche die verschiedenen Tiere betreffenden Daten lesen kann, diese aber ohne die tierspezifische Karte, die vorangehend beschrieben wurde, nicht verändern kann.

Die Betreiber der Zertifizierungsstelle sind ebenfalls im Besitz des privaten und des öffentlichen tierspezifischen Codes und haben volle Zugriffsberechtigung für alle Datenteile.

Dritten Personen kann der Zugang zu den Daten ermöglicht werden, indem der Besitzer (oder die Zertifizierungsstelle) diesen entweder zeitlich begrenzt oder permanent das Lesen der Daten gestattet, beispielsweise durch Vergabe eines Paßworts, und diesen den öffentlichen tierspezifischen Schlüssel zur Verfügung stellt. Weiterhin kann bestimmten Benutzern, beispielsweise Tierärzten, gestattet sein, bestimmte Daten, z. B. Impfdaten, Untersuchungsdaten usw., zu ändern oder neu zu schreiben, wobei diese Benutzer dann die von ihnen neu geschriebenen oder geänderten Daten mit einem für sie spezifischen privaten Schlüssel digital signieren, z. B. durch Verschlüsselung des Wertes einer entsprechenden Einwegfunktion. Wenn diese Daten geändert werden, erzeugt die Zertifizierungsstelle mit dem tierspezifischen privaten Schlüssel eine zweite Signatur in Form des codierten Wertes einer Einwegfunktion,

um die Authentizität der Zuordnung der eingeschriebenen Daten zu dem entsprechenden Tier zu bestätigen.

Es kann jedoch auch vorgesehen sein, daß ein Dritter nur dann auf die Daten zugreifen kann und diese lesen und/oder ändern kann, wenn er gleichzeitig die tierspezifische Chipkarte des Besitzers durch Einschieben in ein entsprechendes Lesegerät zur Autorisierung verwendet. In diesem Fall kann er nur dann auf die bei der Zertifizierungsstelle gespeicherten Daten zugreifen, wenn ihm diese Chipkarte ausgehändigt worden ist und er somit von dem Besitzer autorisiert worden ist.

Bezug nehmend auf das Beispiel eines Tierarztes, welcher eine Schreibberechtigung für Daten bei der Zertifizierungsstelle hat, soll der Zugriff von Dritten noch näher erläutert werden.

Der Tierarzt verfügt über einen privaten und einen öffentlichen Schlüssel, die ihm von der Zertifizierungsstelle und oder nach dem Gesetz zur digitalen Signatur zugewiesen sind. In dem von der Zertifizierungsstelle eingerichteten elektronischen Register ist eine Datei („Registerblatt“) für Behandlungsdaten eingerichtet. Der Tierarzt erhält eine Leseberechtigung für die Stammdaten, wie Geburtsdatum, Abstammungsdatum etc. und eine Zugriffsberechtigung zum Schreiben und Lesen von Impfdaten und zum Schreiben von Behandlungsdaten, wobei das Recht zum Lesen von Behandlungsdaten, welche nicht auf seine Tätigkeit zurückgehen, beschränkt sein kann.

Bei einer Behandlung händigt der Tierbesitzer dem Tierarzt die dem Tier zugeordnete tierspezifische Chipkarte aus, der mit Hilfe dieser Karte eine Verbindung zu der Zertifizierungsstelle aufbaut. Das Auslesen der Zertifikatsinformationen und Übermitteln von auf der tierspezifischen Karte gespeicherten Daten, wie dem gespeicherten öffentlichen tierspezifischen Schlüssel und ein Paßwort, zu der Zertifizierungsstelle, eröffnet den Zugang zu den betreffend das konkrete Tier gespeicherten Daten bei der Zertifizierungsstelle. Zum Lesen bzw. Schreiben der Daten muß der Tierarzt sich noch einmal persönlich identifizieren. Dies kann dadurch erfolgen, daß Daten von einer dem Tierarzt zugeordneten Chipkarte übermittelt werden oder in dem Chipkartenlesegerät oder dem Computer des Tierarztes sicher abgespeicherte Daten automatisch zu der zentralen Stelle übermittelt werden. Bei der Kommunikation zwischen dem Tierarzt und der Zertifizierungsstelle können die üblichen Techniken einer sicheren Ver-

bindung verwendet werden. Z. B. kann mit Hilfe eines asymmetrischen Schlüsselpaares ein für die Sitzung speziell generierter symmetrischer Sitzungsschlüssel ausgetauscht werden, mit welchem alle Kommunikationen zwischen dem Tierarzt und der Zertifizierungsstelle während der Sitzung verschlüsselt werden.

Wenn sowohl eine Authorisierung betreffend das Tier als auch eine Authorisierung des Tierarztes erfolgt ist, kann der Tierarzt die ihm zugänglichen Daten in dem Register der Zertifizierungsstelle lesen bzw., soweit gestattet, verändern. Der Tierarzt versieht die von ihm geänderten oder neu geschriebenen Daten mit einer digitalen Signatur.

Auch eine Kommunikation in umgekehrter Richtung, beispielsweise zur Überweisung von Krankendaten, ist möglich. Dabei wird die entsprechende Nachricht entweder mit dem tierspezifischen privaten Schlüssel oder mit dem privaten Schlüssel des Tierarztes bzw. dem öffentlichen Schlüssel des Empfängers verschlüsselt. Alternativ wird die Nachricht im Klartext übersandt und zum Überprüfen der Authentizität wird eine Signatur, z. B. der Wert einer auf die Nachricht angewandten Einwegfunktion, verschlüsselt mit dem tierspezifischen privaten Schlüssel oder mit dem privaten Schlüssel des Tierarztes, erzeugt und der Nachricht angehängt.

Das vorangehend beschriebene Verfahren kann z. B. zur Identifizierung von Tieren bei Zuchtschauen verwendet werden. Der Tierbesitzer übermittelt zur Anmeldung des Tieres die das Tier identifizierende genetische Information, die dem öffentlichen tierspezifischen Schlüssel, wie vorangehend erläutert, zugrunde liegt, sowie den öffentlichen tierspezifischen Schlüssel, der auf der Chipkarte angegeben ist, oder eine andere Information, welche die Chipkarte der genetischen Information zuordnet. Beim Eintreffen des Tieres auf der Zuchtschau wird das Tier anhand der übersandten genetischen Information identifiziert. Auf der Grundlage des auf der Chipkarte gespeicherten oder abgedruckten Zertifikats wird überprüft, daß der angegebene öffentliche Schlüssel tatsächlich zu der angegebenen genetischen Information gehört, so daß die authentische Zuordnung der Chipkarte zu dem vorgeführten Tier hergestellt wird. Mit der solchermaßen verifizierten Chipkarte kann dann auf die Daten bei der Zertifizierungsstelle zugegriffen werden. Können die Daten bei der Zertifizierungsstelle mit dem auf der Chipkarte abgespeicherten Schlüssel entschlüsselt werden, ist sichergestellt, daß das vorgeführte Tier den bei der Zertifizierungsstelle gespeicherten Daten entspricht.

In ähnlicher Weise kann auch bei geschäftlichen Transaktionen betreffend das Tier, z. B. bei Tierverkäufen, vorgegangen werden. Auch in diesem Fall wird der öffentliche Schlüssel zusammen mit der das Tier identifizierenden genetischen Information übermittelt. Anstelle des öffentlichen Schlüssels kann auch eine andere Information übermittelt werden, welche die eindeutige Zuordnung einer vorzuliegenden Chipkarte zu der übermittelten genetischen Information herstellt. Sofern die Chipkarte die Zuordnung der gespeicherten Daten, insbesondere des gespeicherten Codes, zu der genetischen Information selbsttätig überprüft, reicht auch die Angabe der genetischen Information allein zur Authentifizierung der Karte aus.

Verschiedene Abwandlungen der vorangehend beschriebenen Vorgehensweise sind möglich. Es können z. B. andere Verschlüsselungsverfahren verwendet werden. Zugriffsberechtigungen, insbesondere Lese- oder Schreibrechte können unterschiedlich geregelt sein.

Informationen betreffend die Gewinnung der genetischen Information, der Zuordnung dieser Information zu einem öffentlichen Schlüssel etc. müssen nicht auf einer Chipkarte gespeichert werden, sondern können auch auf andere Weise kommuniziert werden.

Das Verfahren kann als Internet-Marktplatz, z. B. zum elektronischen Tierhandel oder zur elektronischen Tierversteigerung, ausgebildet werden. Dabei werden bestimmte Informationen der Referenzdatensätze oder allgemeiner der bei der Zertifizierungsstelle gespeicherten Daten betreffend die registrierten Tiere und/oder Materialien über Suchfunktionen zugänglich gemacht. Der Marktplatz kann offen sein, wobei die Absicherung der Datenübertragung durch standardmäßige Verfahren erfolgen kann. Alternativ kann der Zugang zu den Informationen allgemein oder auch nur für bestimmte Informationen auf berechtigte Benutzer beschränkt sein.

Im Rahmen des Aufbaus einer genetischen Zertifizierungsstelle können spezifische genetische Informationen der Referenzdatensätze als elektronische oder geschriebene Zertifikate für die jeweiligen Tiere bzw. Materialien ausgegeben werden, insbesondere als Zertifikat für sonstige Eigenschaften und/oder Merkmale.

Schließlich kann das erfindungsgemäße Verfahren zum Aufbau einer standardisierten Tierdatenbank verwendet werden, bei welchem nicht mehr die genetische Information (der „genetische Fingerabdruck“) die das Tier identifizierenden Daten bildet, sondern vielmehr der dieser Information zugeordnete Schlüssel. Die Verfahren, die derzeit zum Erstellen eines „genetischen Fingerabdrucks“ verwendet werden, sind unterschiedlich, so daß ein und dasselbe Tier mehreren „genetischen Fingerabdrücken“ entsprechen kann, je nach dem, welches Verfahren verwendet wurde. Dementsprechend ist es derzeit schwierig, anhand der genetischen Information verschiedene Datenbanken auf Daten zu durchsuchen, die sich auf dasselbe Tier beziehen. Im Rahmen der Erfindung ist das Verfahren zur Gewinnung des genetischen Fingerabdrucks unwichtig, solange jedem Tier nur ein einziger individuell zugeordneter Schlüssel (oder eine andere digitale Information) zugewiesen wird; primäres Suchkriterium ist der tierspezifische Code oder Schlüssel. Die eindeutige Verbindung zwischen Schlüssel und der spezifischen genetischen Information erfolgt durch ein Zertifikat, welches das Verfahren, mit welchem der genetische Fingerabdruck ermittelt wurde, und den zugeordneten Schlüssel benennt, wobei dieses Zertifikat stets zusammen mit dem Schlüssel verfügbar ist und entweder zusammen mit diesem gespeichert ist oder jederzeit über einen Server abrufbar ist.

Die in der vorangehenden Beschreibung und den Ansprüchen offenbarten Merkmale der Erfindung können sowohl alleine als auch in beliebiger Kombination für die Verwirklichung der Erfindung in ihren verschiedenen Ausführungsformen wesentlich sein.

---

Patentansprüche

---

1. Verfahren zum Nachweis der Abstammung und/oder zur Identifizierung von Tieren oder von biologischem Material von Tieren und Organismen, welches die folgenden Schritte umfaßt:
  - Speichern von Identifikationsdaten in Form einer verschlüsselten Nachricht, welche in einer eindeutigen vorgegebenen Beziehung zu einer genetischen Information steht, welche ein Tier oder das biologische Material eindeutig identifiziert, auf einem Datenträger,
  - Überprüfen der Identifikationsdaten daraufhin, ob diese in der vorgegebenen Beziehung zu der genetischen Information stehen.
2. Verfahren nach Anspruch 1, daß die genetischen Informationen von einem oder mehreren Tieren oder von biologischem Material von einem oder mehreren Tieren oder Organismen bestimmt und auf einem Speichermedium als Referenzdatensätze abgespeichert werden.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß auf dem Datenträger den Identifikationsdaten zugeordnet weitere Daten betreffend das zu identifizierende Tier bzw. das zu identifizierende biologische Material gespeichert sind.
4. Verfahren nach Anspruch 1 bis 3, dadurch gekennzeichnet, daß die Identifikationsdaten eine verschlüsselte Nachricht enthalten, welche mit einem dem individuellen Tier oder Material eindeutig zugeordneten Code verschlüsselt ist.
5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß die verschlüsselte Nachricht den Wert einer Einwegfunktion (Hash) enthält, der sich ergibt, wenn diese Einwegfunktion auf weitere auf dem Datenträger gespeicherte Daten betreffend das zu identifizierende Tier bzw. das zu identifizierende biologische Material angewendet wird.

6. Verfahren nach einem Ansprüche 1 bis 5, dadurch gekennzeichnet, daß eine verschlüsselte Nachricht eine das Tier bzw. das Material eindeutig identifizierende genetische Information umfaßt.
7. Verfahren nach einem der Ansprüche 3 bis 6, dadurch gekennzeichnet, daß die Identifikationsdaten verschlüsselte Daten betreffend den Speicherort und/oder den Inhalt von weiteren Daten betreffend das den Identifikationsdaten zugeordneten Tiers umfassen.
8. Verfahren nach einem der Ansprüche 4 bis 7, dadurch gekennzeichnet, daß die Identifikationsdaten eine Nachricht umfassen, die mit einem Code verschlüsselt wird, welcher auf der Grundlage einer Ziffernfolge in einer vorbestimmten eindeutigen Weise generiert ist, welche einer genetischen Information, welche das Tier bzw. das Material eindeutig identifiziert, eindeutig zugeordnet ist.
9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß die Ziffernfolge zumindest einen Teil des Codes bildet.
10. Verfahren nach Anspruch 8 oder 9, dadurch gekennzeichnet, daß der Schlüssel ein symmetrischer Schlüssel ist.
11. Verfahren nach Anspruch 8 oder 9, dadurch gekennzeichnet, daß die Nachricht auf der Grundlage des privaten Schlüssels eines asymmetrischen Schlüsselpaares verschlüsselt ist, wobei zumindest ein Teil des öffentlichen Schlüssels in einer vorgegebenen Beziehung zu der das Tier bzw. das Material identifizierenden genetischen Information steht.
12. Verfahren nach Anspruch 11, daß der öffentliche Schlüssel aus einem für das Tier bzw. das Material spezifischen Anteil und einem benutzerspezifischen Anteil besteht.

13. Verfahren nach einem der Ansprüche 8 bis 12, dadurch gekennzeichnet, daß die identifizierenden Daten zusätzlich mit einem benutzerspezifischen Schlüssel verschlüsselt werden.
14. Verfahren nach einem der Ansprüche 8 bis 13, dadurch gekennzeichnet, daß zumindest ein Teil der Daten auf dem Datenträger, welche den Identifikationsdaten zugeordnet sind, mit einem Code verschlüsselt sind, der verschieden von dem Code ist, mit welchem die Identifikationsdaten verschlüsselt sind.
15. Verfahren nach einem der Ansprüche 8 bis 14, dadurch gekennzeichnet, daß der Schlüssel zum Entschlüsseln der in den Identifikationsdaten enthaltenen Nachricht auf einem Träger eines Chips zum Kommunizieren mit einer Datenverarbeitungsanlage über eine Schnittstelle, insbesondere auf einer Chipkarte, gespeichert ist.
16. Verfahren nach Anspruch 15, dadurch gekennzeichnet, daß der Chip eine Einrichtung zum Entschlüsseln von Nachrichten aufweist.
17. Verfahren nach Anspruch 15 oder 16, dadurch gekennzeichnet, daß der die Nachricht der Identifikationsdaten codierende Schlüssel ein asymmetrischer Schlüssel ist, der zugehörige private Schlüssel auf dem Chip gespeichert ist und der Chip eine Einrichtung zum Verschlüsseln von Nachrichten mit dem privaten Schlüssel aufweist.
18. Verfahren nach einem der Ansprüche 15 bis 17, dadurch gekennzeichnet, daß der Chip eine Schnittstelle zum Eingeben von digitalisierter genetischer Information und eine Einrichtung zum Überprüfen der Zuordnung des gespeicherten Codes zu einer eingegebenen digitalisierten genetischen Information enthält.
19. Verfahren nach Anspruch 18, dadurch gekennzeichnet, daß die Vergleichseinrichtung die eingegebene digitalisierte genetische Information mit einem abgespeicherten Wert für diese Information vergleicht und ein Ausgangssignal abgibt, welches anzeigt, ob eine Übereinstimmung vorliegt oder nicht.

20. Verfahren nach Anspruch 18, dadurch gekennzeichnet, daß die Vergleichseinrichtung auf der Grundlage der eingegebenen digitalisierten genetischen Information und einer abgespeicherten Zuordnung einer digitalisierten genetischen Information, welche das Tier bzw. das Material eindeutig identifiziert, zu dem abgespeicherten Schlüssel einen der eingegebenen Information zugeordneten Schlüssel bestimmt, den so bestimmten Schlüssel mit dem abgespeicherten Schlüssel vergleicht und ein Ausgangssignal abgibt, welches anzeigt, ob der aufgrund der Eingabe bestimmte Schlüssel mit dem abgespeicherten Schlüssel übereinstimmt oder nicht.
21. Verfahren nach einem der Ansprüche 15 bis 20, dadurch gekennzeichnet, daß in dem Chip einen oder mehrere Benutzer identifizierende Informationen gespeichert sind und die Entschlüsselungs- bzw. Verschlüsselungseinrichtung nur dann aktiviert wird, wenn über eine Eingabeeinrichtung eine für einen Benutzer als Identifizierung gespeicherte Information eingegeben wird.
22. Verfahren nach einem der Ansprüche 8 bis 21, dadurch gekennzeichnet, daß der Code zum Entschlüsseln von codierter Information, die in den Identifikationsdaten enthalten ist, in einem zentralen Rechner gespeichert ist.
23. Verfahren nach Anspruch 22, dadurch gekennzeichnet, daß der Rechner aufgrund einer eingegebenen oder vorgegebenen genetischen Information den zugehörigen Schlüssel bestimmt und diesen Schlüssel auf die Identifikationsdaten anwendet.
24. Verfahren nach Anspruch 23, dadurch gekennzeichnet, daß der zentrale Rechner nach der Entschlüsselung überprüft, ob vorgegebene Zeichenfolgen in dem entschlüsselten Klartext vorhanden sind und ein entsprechendes Ausgangssignal an einen Benutzer abgibt.
25. Verfahren nach Anspruch 23 oder 24, dadurch gekennzeichnet, daß die auf dem Datenträger gespeicherte Information sowie gegebenenfalls eine vorbestimmte, das Tier bzw. das Material eindeutig identifizierende genetische Information zu dem zentralen Rechner übermittelt wird,

26. Verfahren nach einem der Ansprüche 1 bis 24, dadurch gekennzeichnet, daß der Datenträger mit den auf das Tier bzw. das Material bezogenen Daten auf einem zentralen Rechner installiert ist.
27. Verfahren nach Anspruch 26, dadurch gekennzeichnet, daß zumindest ein Teil der Daten zugriffsgeschützt ist und die Zugriffsberechtigung für verschiedene Benutzer des zentralen Rechners verschieden ist.
28. Verfahren nach Anspruch 27, dadurch gekennzeichnet, daß für einen Teil der Benutzer ein Zugriff auf zumindest einen Teil der gespeicherten Daten nur dann möglich ist, wenn gleichzeitig ein vorbestimmter weiterer Benutzer bei dem zentralen Rechner angemeldet ist.
29. Verfahren nach einem der Ansprüche 26 bis 28, dadurch gekennzeichnet, daß ein Zugriff auf zumindest einen Teil der gespeicherten Daten nur dann möglich ist, wenn der Rechner anhand der auf einem Chip, insbesondere auf einer Chipkarte, gespeicherten Daten die Zugriffsberechtigung überprüft hat.
30. Verfahren nach einem der Ansprüche 27 bis 29, dadurch gekennzeichnet, daß der Rechner so eingerichtet ist, daß ein Schreiben von Benutzern in die abgespeicherten, auf das Tier bzw. das Material bezogenen Daten nur zusammen mit einer digitalen Signatur des Benutzers möglich ist.
31. Verfahren nach einem der Ansprüche 26 bis 30, dadurch gekennzeichnet, daß ein tier-spezifisches Paar von asymmetrischen Schlüsseln zum Austausch eines Sitzungsschlüssels für die Kommunikation eines Benutzers mit dem zentralen Rechner verwendet wird.
32. Verfahren zum Generieren von Daten, welche zu einem individuellen Tier nachprüfbar in einer eindeutigen Beziehung stehen, welches umfaßt:
  - Erzeugen von Identifikationsdaten in Form einer verschlüsselten Nachricht, welche in einer eindeutigen vorgegebenen Beziehung zu einer genetischen In-

formation steht, welche ein Tier oder das biologische Material eindeutig identifiziert.

- Speichern der Identifikationsdaten auf einem Datenträger.

33. Verfahren nach Anspruch 32, dadurch gekennzeichnet, daß die Identifikationsdaten eine verschlüsselte Nachricht enthalten, welche mit einem dem individuellen Tier eindeutig zugeordneten Schlüssel verschlüsselt ist.
34. Verfahren nach Anspruch 33, dadurch gekennzeichnet, daß die verschlüsselte Nachricht den Wert einer Einwegfunktion (Hash) enthält, der sich ergibt, wenn diese Einwegfunktion auf weitere auf dem Datenträger gespeicherte Daten betreffend das zu identifizierende Tier bzw. dem zu identifizierenden biologischen Material angewendet wird.
35. Verfahren nach einem der Ansprüche 32 bis 34, dadurch gekennzeichnet, daß die Identifikationsdaten eine Nachricht umfassen, die mit einem Code verschlüsselt ist, welcher auf der Grundlage einer Ziffernfolge in einer vorbestimmten eindeutigen Weise generiert ist, welche einer genetischen Information, welche das Tier bzw. das Material eindeutig identifiziert, eindeutig zugeordnet ist.
36. Verfahren nach Anspruch 35, dadurch gekennzeichnet, daß der Schlüssel ein symmetrischer Schlüssel ist.
37. Verfahren nach Anspruch 35, dadurch gekennzeichnet, daß die Information auf der Grundlage eines asymmetrischen Schlüsselpaares verschlüsselt ist, wobei zumindest ein Teil des öffentlichen Schlüssels in einer vorgegebenen Beziehung zu der genetischen Information steht.
38. Chipträger zur Identifizierung von Tieren, der zur Kommunikation zwischen einem Chip auf dem Chipträger und einem Rechner über eine Schnittstelle eingerichtet ist, insbesondere Chipkarte, dadurch gekennzeichnet, daß auf dem Chip ein Schlüssel gespeichert ist, der zu einer für das individuelle Tier spezifischen genetischen Information in einer eindeutigen vorgegebenen Beziehung steht.

39. Chipträger nach Anspruch 38, dadurch gekennzeichnet, daß der Chip einen Prozessor zum Entschlüsseln von Nachrichten mit dem gespeicherten Schlüssel aufweist.
40. Chipkarte nach einem der Ansprüche 38 oder 39, dadurch gekennzeichnet, daß der Chip eine Schnittstelle zum Eingeben von digitalisierter genetischer Information und eine Vergleichseinrichtung zum Überprüfen der Zuordnung des gespeicherten Codes zu einer eingegebenen digitalisierten genetischen Information enthält.
41. Computersystem zur Durchführung eines Verfahrens nach einem der Ansprüche 1 bis 31, gekennzeichnet durch einen zentralen Rechner, welcher einen Datenträger aufweist, auf dem Identifikationsdaten gespeichert sind, die in einer eindeutigen vorgegebenen Beziehung zu einer genetischen Information stehen, welche ein Tier oder das biologische Material eindeutig identifiziert.



# INTERNATIONAL SEARCH REPORT

Internal Application No

PCT/DE 99/01937

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 A01K11/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 A01K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No.        |
|----------|--|------------------------------|
| X        | DE 196 29 531 A (PAETSCH RALPH)<br>29 January 1998 (1998-01-29)<br><br>the whole document<br>---                               | 1-4, 6,<br>26, 32,<br>38, 41 |
| E        | EP 0 941 655 A (NEDAP NV)<br>15 September 1999 (1999-09-15)<br>column 1, line 3 -column 2, line 22;<br>claims<br>---           | 1-3, 32,<br>38               |
| X        | EP 0 646 313 A (SURGE MIYAWAKI CO LTD)<br>5 April 1995 (1995-04-05)<br>column 1, line 15 -column 6, line 58<br>---<br><br>-/-- | 1-3, 32,<br>41               |

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

### Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

16 December 1999

Date of mailing of the international search report

22/12/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040. Tx. 31 651 epo nl.  
Fax: (+31-70) 340-3016

Authorized officer

Acerbis, G

## INTERNATIONAL SEARCH REPORT

Internat: Application No  
PCT/DE 99/01937

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
|----------|--|-----------------------|
| A        | PATENT ABSTRACTS OF JAPAN<br>vol. 1998, no. 11,<br>30 September 1998 (1998-09-30)<br>& JP 10 151125 A (CORP<br>MIYUKI:KK;ATSUKUSU:KK),<br>9 June 1998 (1998-06-09)<br>abstract; figures<br>---                                     | 1-41                  |
| A        | US 4 475 481 A (CARROLL GARY T)<br>9 October 1984 (1984-10-09)<br>column 1, line 10 -column 3, line 36<br>---  | 1-41                  |
| A        | EP 0 299 557 A (NEDAP NV)<br>18 January 1989 (1989-01-18)<br>abstract<br>---   | 1                     |
| A        | EP 0 307 335 A (HADJADJ JACQUES)<br>15 March 1989 (1989-03-15)<br>the whole document<br>---  | 1                     |
| A        | HELLMAN M E: "The mathematics of<br>public-key cryptography"<br>SCIENTIFIC AMERICAN,US,SCIENTIFIC AMERICAN<br>INC. NEW YORK,<br>vol. 241, no. 2, page 130-139-139<br>XP002097245<br>ISSN: 0036-8733<br>the whole document<br>----- |                       |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Internati Application No

PCT/DE 99/01937

| Patent document<br>cited in search report | Publication<br>date | Patent family<br>member(s) | Publication<br>date |
|---|---------------------|----------------------------|---------------------|
| DE 19629531 A                             | 29-01-1998          | NONE                       |                     |
| EP 0941655 A                              | 15-09-1999          | NL 1008540 C               | 10-09-1999          |
| EP 0646313 A                              | 05-04-1995          | JP 6276877 A               | 04-10-1994          |
|   |                     | WO 9422295 A               | 13-10-1994          |
|   |                     | US 5697384 A               | 16-12-1997          |
| JP 10151125 A                             | 09-06-1998          | NONE                       |                     |
| US 4475481 A                              | 09-10-1984          | AU 2264383 A               | 22-05-1984          |
|   |                     | CA 1206532 A               | 24-06-1986          |
|   |                     | EP 0125287 A               | 21-11-1984          |
|   |                     | WO 8401688 A               | 10-05-1984          |
| EP 0299557 A                              | 18-01-1989          | NL 8701541 A               | 01-02-1989          |
|   |                     | CN 1030647 A               | 25-01-1989          |
|   |                     | DD 292722 A                | 08-08-1991          |
|   |                     | DE 3865761 A               | 28-11-1991          |
|   |                     | DK 364888 A                | 02-01-1989          |
|   |                     | JP 1030526 A               | 01-02-1989          |
|   |                     | SU 1704610 A               | 07-01-1992          |
| EP 0307335 A                              | 15-03-1989          | FR 2620546 A               | 17-03-1989          |
|   |                     | AT 88029 T                 | 15-04-1993          |
|   |                     | DE 3880058 A               | 13-05-1993          |



## A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 A01K11/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

## B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 A01K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

## C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile                             | Betr. Anspruch Nr.           |
|-----------|--|------------------------------|
| X         | DE 196 29 531 A (PAETSCH RALPH)<br>29. Januar 1998 (1998-01-29)<br><br>das ganze Dokument<br>---                               | 1-4, 6,<br>26, 32,<br>38, 41 |
| E         | EP 0 941 655 A (NEDAP NV)<br>15. September 1999 (1999-09-15)<br>Spalte 1, Zeile 3 - Spalte 2, Zeile 22;<br>Ansprüche<br>---    | 1-3, 32,<br>38               |
| X         | EP 0 646 313 A (SURGE MIYAWAKI CO LTD)<br>5. April 1995 (1995-04-05)<br>Spalte 1, Zeile 15 - Spalte 6, Zeile 58<br>---<br>-/-- | 1-3, 32,<br>41               |



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

Besondere Kategorien von angegebenen Veröffentlichungen

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

16. Dezember 1999

Absenddatum des internationalen Recherchenberichts

22/12/1999

Name und Postanschrift der Internationalen Recherchenbehörde  
Europäisches Patentamt, P. B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.  
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Acerbis, G

| C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN |  |                    |
|--|--|--------------------|
| Kategorie  | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile   | Betr. Anspruch Nr. |
| A  | PATENT ABSTRACTS OF JAPAN<br>vol. 1998, no. 11,<br>30. September 1998 (1998-09-30)<br>& JP 10 151125 A (CORP<br>MIYUKI:KK;ATSUKUSU:KK),<br>9. Juni 1998 (1998-06-09)<br>Zusammenfassung; Abbildungen<br>---                        | 1-41               |
| A  | US 4 475 481 A (CARROLL GARY T)<br>9. Oktober 1984 (1984-10-09)<br>Spalte 1, Zeile 10 -Spalte 3, Zeile 36<br>---   | 1-41               |
| A  | EP 0 299 557 A (NEDAP NV)<br>18. Januar 1989 (1989-01-18)<br>Zusammenfassung<br>---  | 1                  |
| A  | EP 0 307 335 A (HADJADJ JACQUES)<br>15. März 1989 (1989-03-15)<br>das ganze Dokument<br>---  | 1                  |
| A  | HELLMAN M E: "The mathematics of<br>public-key cryptography"<br>SCIENTIFIC AMERICAN,US,SCIENTIFIC AMERICAN<br>INC. NEW YORK,<br>Bd. 241, Nr. 2, Seite 130-139-139<br>XP002097245<br>ISSN: 0036-8733<br>das ganze Dokument<br>----- |                    |

# INTERNATIONALER RESEARCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internati 35 Aktenzeichen

PCT/DE 99/01937

| Im Recherchenbericht<br>angeführtes Patentdokument | Datum der<br>Veröffentlichung | Mitglied(er) der<br>Patentfamilie | Datum der<br>Veröffentlichung |
|--|-------------------------------|-----------------------------------|-------------------------------|
| DE 19629531 A                                      | 29-01-1998                    | KEINE                             |                               |
| EP 0941655 A                                       | 15-09-1999                    | NL 1008540 C                      | 10-09-1999                    |
| EP 0646313 A                                       | 05-04-1995                    | JP 6276877 A                      | 04-10-1994                    |
|  |                               | WO 9422295 A                      | 13-10-1994                    |
|  |                               | US 5697384 A                      | 16-12-1997                    |
| JP 10151125 A                                      | 09-06-1998                    | KEINE                             |                               |
| US 4475481 A                                       | 09-10-1984                    | AU 2264383 A                      | 22-05-1984                    |
|  |                               | CA 1206532 A                      | 24-06-1986                    |
|  |                               | EP 0125287 A                      | 21-11-1984                    |
|  |                               | WO 8401688 A                      | 10-05-1984                    |
| EP 0299557 A                                       | 18-01-1989                    | NL 8701541 A                      | 01-02-1989                    |
|  |                               | CN 1030647 A                      | 25-01-1989                    |
|  |                               | DD 292722 A                       | 08-08-1991                    |
|  |                               | DE 3865761 A                      | 28-11-1991                    |
|  |                               | DK 364888 A                       | 02-01-1989                    |
|  |                               | JP 1030526 A                      | 01-02-1989                    |
|  |                               | SU 1704610 A                      | 07-01-1992                    |
| EP 0307335 A                                       | 15-03-1989                    | FR 2620546 A                      | 17-03-1989                    |
|  |                               | AT 88029 T                        | 15-04-1993                    |
|  |                               | DE 3880058 A                      | 13-05-1993                    |



1

1